Fortanix

Solution Brief

Fortanix Confidential-AI (C-AI)

Unlock the power of private data and build smarter AI models

Addressing the Challenges of Using Private Data in AI

Fortanix Confidential AI (C-AI) enables data teams, in regulated, privacy sensitive industries such as healthcare and financial services, to utilize private data for developing and deploying better AI models, using Confidential Computing.

The potential of AI and data analytics in augmenting business growth and advancement of solutions and services through data-driven innovation is well known. And that's why AI adoption has been skyrocketing over the years. According to **Gartner**, by the end of 2024, 75% of enterprises will shift from piloting to operationalizing AI, driving a 5X increase in streaming data and analytics infrastructures. But MLOps often depend upon data that is sensitive and holds Personally Identifiable Information which is often subject to usage restrictions and carries compliance obligations. AI efforts can fail to move out of the lab if data teams are unable to use this sensitive data.

75% of enterprises will shift from piloting to operationalizing AI by the end of 2024.

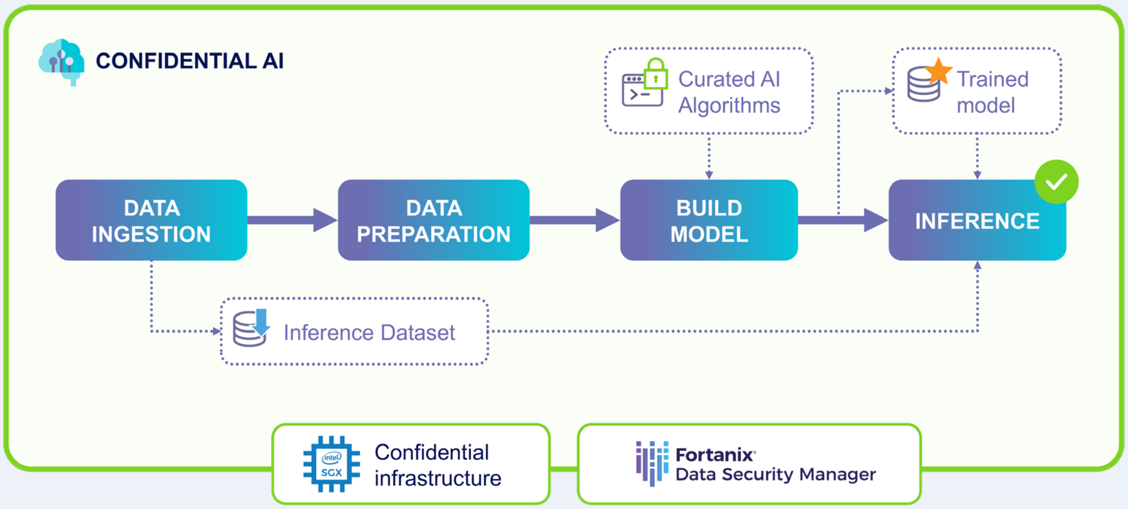
Realizing the full potential of AI is possible only if critical issues like data privacy and secure use of private information are addressed. And for most organizations within heavily regulated industries like healthcare and BFSI, large portions of such data still remains out of reach due to privacy concerns. For example: obtaining sufficiently large and meaningful clinical-trial data sets for training and predicting healthcare treatment outcomes is often challenging as its governed by privacy regulations like HIPAA.

Unlocking the full power of private data can only be done in a highly secure trusted execution environments. The emergence of Confidential Computing as a new security paradigm offers data scientists with a practical solution to the problem of protecting sensitive private data while being processed.

Solution Overview

Fortanix Confidential-AI had been specifically designed keeping in mind the unique privacy and compliance requirements of regulated industries, as well as the need to protect the intellectual property of the AI models. Fortanix Confidential AI is offered as an easy to use and deploy, software and infrastructure subscription service.

Unlike traditional AI solutions that focus on accelerating modeling processes, Fortanix Confidential AI helps build richer models and protect the IP as well. It alleviates concerns of exposing private data by running datasets in secure enclaves and provides proof of execution in a trusted execution environment for compliance purposes.



Benefits

Build smarter models with more relevant data.

Availability of relevant data is critical to improve existing models or train new models for prediction. Out of reach private data can be accessed and used only within secure environments. Use of confidential computing in various stages ensures that the data can be processed, and models can be developed while keeping the data confidential even when while in use.

Keep models secure and protect intellectual property

Organizations need to protect intellectual property of developed models. With increasing adoption of cloud to host the data and models, privacy risks have compounded. Fortanix Confidential AI makes it easy for a model provider to secure their intellectual property by publishing the algorithm in a secure enclave. The cloud provider insider gets no visibility into the algorithms.

Easily deploy and provision with a managed service

With limited hands-on experience and visibility into technical infrastructure provisioning, data teams need an easy to use and secure infrastructure that can be easily turned on to perform analysis. As a SaaS infrastructure service, Fortanix Confidential AI can be deployed and provisioned at a click of a button with no hands-on expertise required.

Furnish proof of execution to meet the most stringent privacy regulations

Secure infrastructure and audit/log for proof of execution allows you to meet the most stringent privacy regulations across regions and industries.

Get instant project sign-off from security and compliance teams

Get instant project sign-off from your security and compliance teams by relying on the Worlds' first secure confidential computing infrastructure built to run and deploy AI.

Trusted vendor with break through security heritage

Work with the industry leader in Confidential Computing. Fortanix introduced its breakthrough 'runtime encryption' technology that has created and defined this category.

Solution Highlights

Readily available and managed confidential infrastructure

Fortanix C-AI provides a readily available managed Confidential Computing infrastructure that's easy to deploy and provision. The solution is powered on Intel Ice Lake third generation scalable Xeon processors.

Run AI models inside Intel SGX and other enclave technologies

AI models and frameworks are enabled to run inside confidential compute with no visibility for external entities into the algorithms.

Hardware-backed proof of execution and audit logging

The solution offers organizations with hardware backed proofs of execution of confidentiality and data provenance for audit and compliance. Fortanix also provides audit logs to easily verify compliance requirements to support data regulation policies such as GDPR.

Support for a broad set of AI/ML models

AI high performers have standard tool frameworks and development processes in place for developing AI models. Fortanix Confidential-AI supports a range of models such as Yolov 5, Decision Trees, SVM, Linear regression, KNN etc.

Protect data across all stages of MLops

The service provides multiple stages of the data pipeline for an AI project and secures each stage using confidential computing including data ingestion, learning, inference, and fine tuning.

Works with Azure

Fortanix managed and deployed infrastructure works on Azure AKS with SGX enabled nodes

Dataset connectors support data ingestion

Dataset connectors help bring data from Amazon S3 accounts or allow upload of data from local machine.

Add security components like Tokenization and Encryption

Integration with Fortanix Data Security Manager allows organizations to further enhance security through additional components like key management and tokenization.

Some AI Project Use Cases

BY FUNCTION

MARKETING

- Customer-service analytics
- Customer segmentation
- Targeted marketing

RISK MANAGEMENT

- Risk modeling and analytics
- Fraud and debt analytics

STRATEGY AND CORPORATE FINANCE

- Capital allocation
- M&A support

BY INDUSTRY

HEALTHCARE

- Speech analytics and sentiment analysis to provide better tele-customer service in healthcare
- Fraud claim detection for health insurance
- Diagnosing medical conditions in radiology images
- Disease prediction using historical medical data

BANKING

- Abnormalities and trend analysis within financial planning
- Capital market trends and mood analysis
- Fraud detection with ML

INSURANCE

- Churn prediction for customers at risk
- Forecasting of claims and triage analytics
- Underwriting and other automatic workflows

RETAIL

- Purchase pattern analysis and targeted marketing
- Predictive purchase analysis using customer profile data

> *Fortanix is helping accelerate AI deployments in real world settings with its confidential computing technology. The validation and security of AI algorithms using patient medical and genomic data has long been a major concern in the healthcare arena, but it's one that can be overcome thanks to the application of this next-generation technology."*

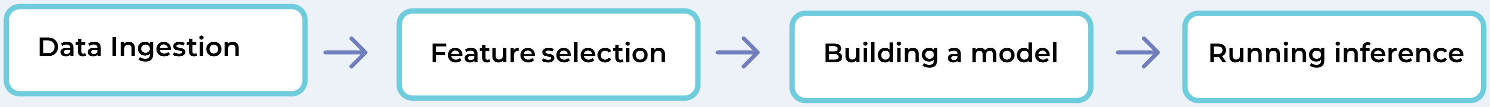
Glen Otero,

Vice President of Scientific Computing at Translational Genomics Research Institute (TGen)

How Does the Solution Work?

Users can perform the following functions inside Confidential AI during the operational phase

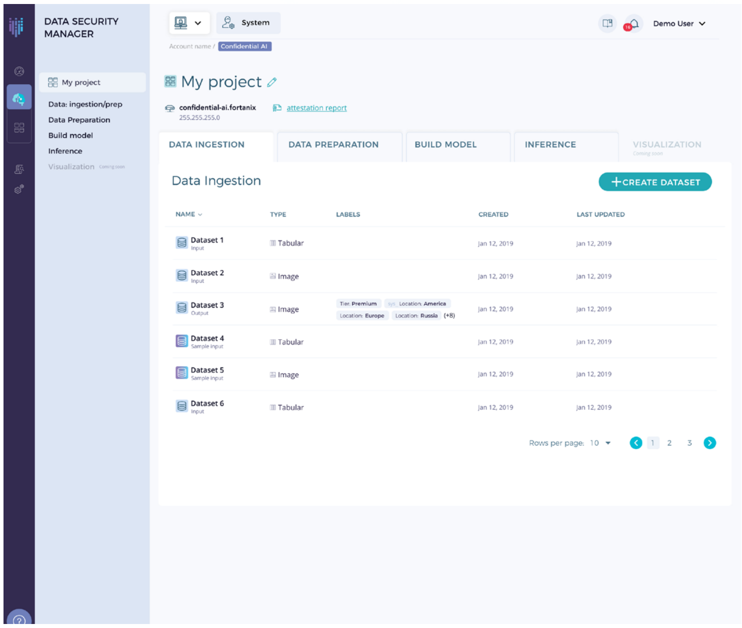
- *Provision Fortanix managed infrastructure for running curated applications as part of account creation*
- *Deploy pre-built curated AI models*
- *Connect datasets from external service and/or upload new datasets in a CSV format*
- *Create Confidential AI projects to create AI workflows*



Data Ingestion → Feature selection → Building a model → Running inference

Data Ingestion:

In Data ingestion phase, the data will be collected either by connecting to an S3 bucket or user can upload their data to the confidential AI platform.

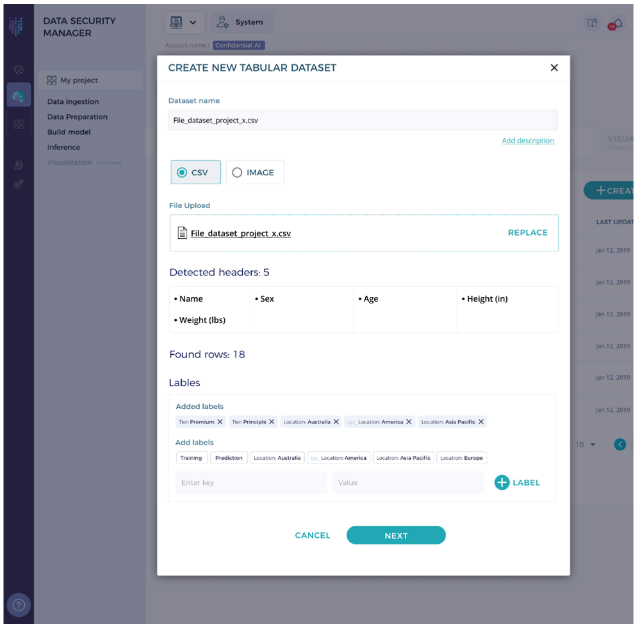


My project

confidential-ai.fortanix 255.255.255.0 attestation report

Data Ingestion

NAME	TYPE	LABELS	CREATED	LAST UPDATED
Dataset 1 Input	Tabular		Jan 12, 2019	Jan 12, 2019
Dataset 2 Input	Image		Jan 12, 2019	Jan 12, 2019
Dataset 3 Output	Image	Tier: Premium sys Location: America Location: Europe Location: Russia (+8)	Jan 12, 2019	Jan 12, 2019
Dataset 4 Sample input	Tabular		Jan 12, 2019	Jan 12, 2019
Dataset 5 Sample input	Image		Jan 12, 2019	Jan 12, 2019
Dataset 6 Input	Tabular		Jan 12, 2019	Jan 12, 2019



CREATE NEW TABULAR DATASET

Dataset name: File_dataset_project_x.csv

● CSV ○ IMAGE

File Upload: File_dataset_project_x.csv

Detected headers: 5

- Name
- Sex
- Age
- Height (in)
- Weight (lbs)

Found rows: 18

Lables

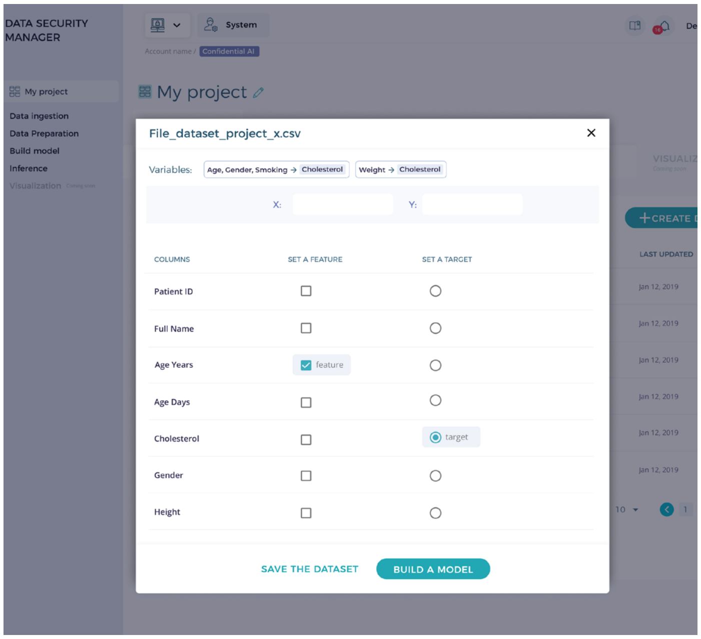
Added labels: Tier: Premium ✕ Tier: Principle ✕ Location: Australia ✕ sys_Location: America ✕ Location: Asia Pacific ✕

Add labels: Training Prediction Location: Australia sys_Location: America Location: Asia Pacific Location: Europe

Enter key | Value

Data preparation:

In this stage, the users can choose the column names as a set of features and targets from the tabular dataset uploaded in the previous stage.

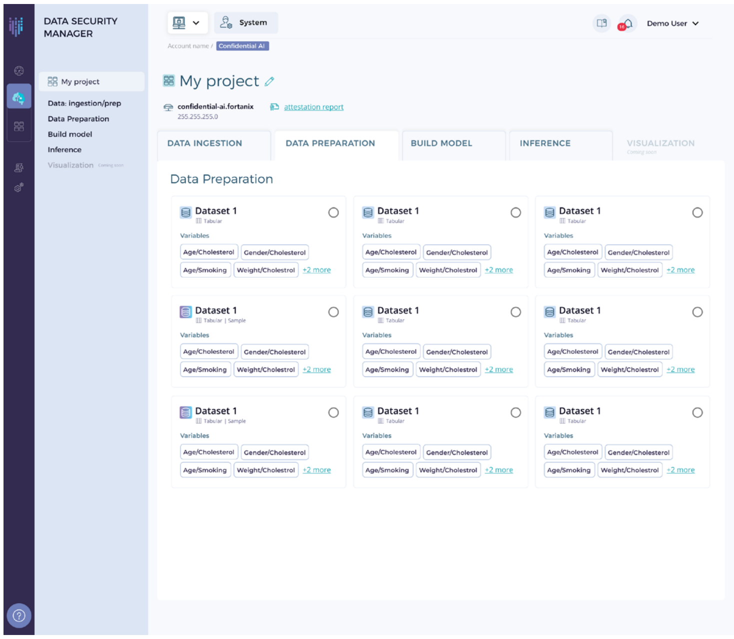


File_dataset_project_x.csv

Variables: Age, Gender, Smoking → Cholesterol   Weight → Cholesterol

X: Y:

COLUMNS	SET A FEATURE	SET A TARGET
Patient ID	□	○
Full Name	□	○
Age Years	☑ feature	○
Age Days	□	○
Cholesterol	□	● target
Gender	□	○
Height	□	○



My project

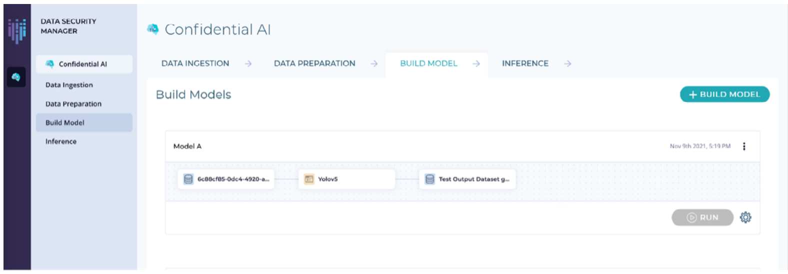
confidential-ai.fortanix 255.255.255.0 attestation report

Data Preparation

Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more
Dataset 1 ○ Tabular | Sample Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more
Dataset 1 ○ Tabular | Sample Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more	Dataset 1 ○ Tabular Variables Age/Cholesterol Gender/Cholesterol Age/Smoking Weight/Cholestrol +2 more

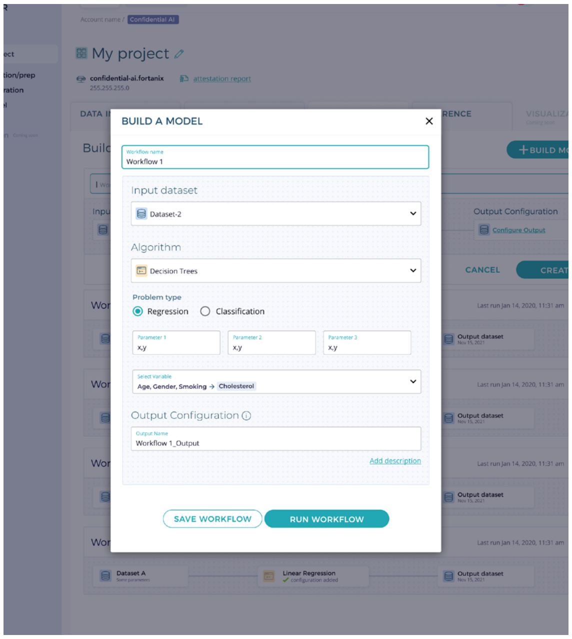
Building a model:

In this stage, the user has the option to build models by running a selection of pre-curated AI algorithms provided by Fortanix. The algorithms supported are: SVM (Support Vector Machines), Yolov5, Decision Trees, KNN, Linear Regression. Each algorithm supports a mode and data type for each mode.



Model A — Nov 9th 2021, 5:19 PM

6c88cf85-0dc4-4920-a... — Yolov5 — Test Output Dataset g...



Workflow name: Workflow 1

Input dataset: Dataset-2

Algorithm: Decision Trees

Problem type: ● Regression ○ Classification

Parameter 1: x,y
Parameter 2: x,y
Parameter 3: x,y

Select Variable: Age, Gender, Smoking → Cholesterol

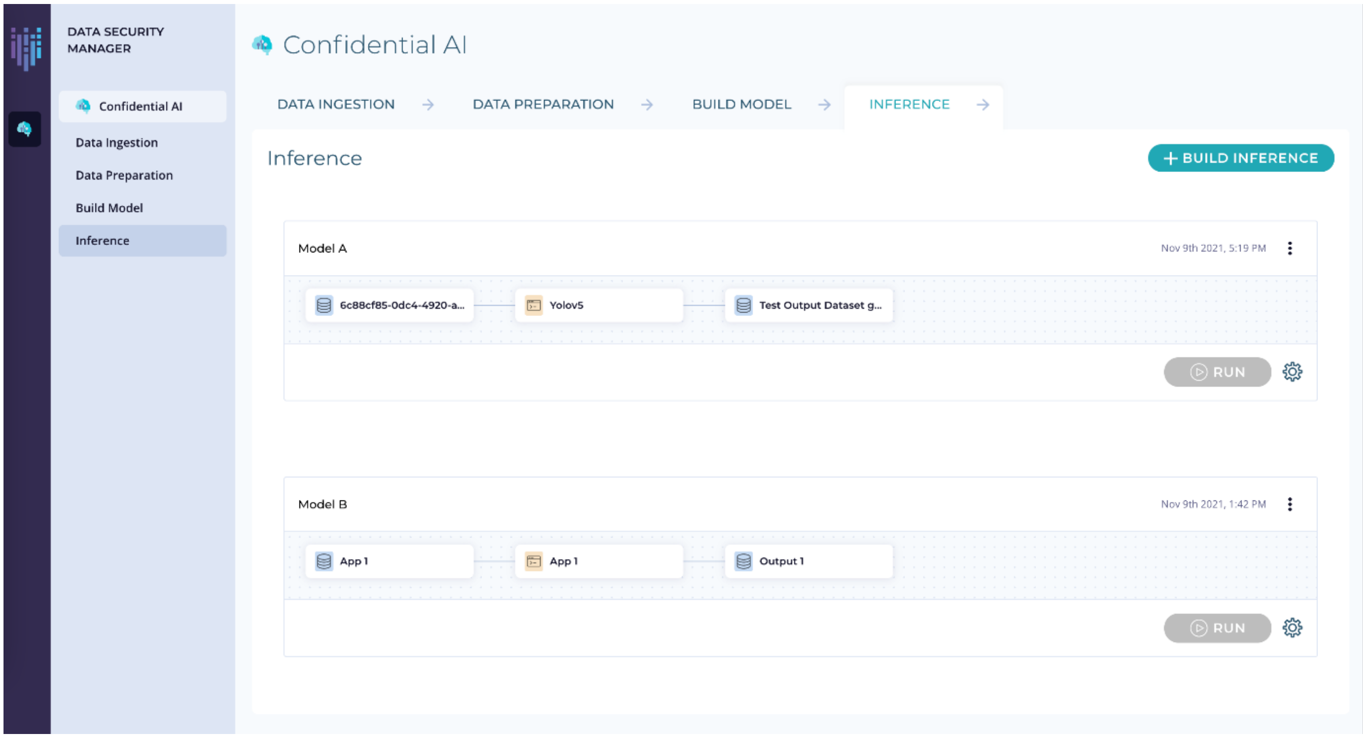
Output Configuration
Output Name: Workflow 1_Output

Last run Jan 14, 2020, 11:31 am

Dataset A (Some parameters) — Linear Regression ✓ configuration added — Output dataset Nov 15, 2021

Running inference:

In this stage, the data (images or tabular) is passed through a machine learning model to identify and predict the output from the data.



Model A — Nov 9th 2021, 5:19 PM

6c88cf85-0dc4-4920-a... — Yolov5 — Test Output Dataset g...

Model B — Nov 9th 2021, 1:42 PM

App 1 — App 1 — Output 1

Talk to our experts for a free assessment of your AI project infrastructure

TAKE A FREE ASSESSMENT NOW!

About Fortanix

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks. For more information, see **www.fortanix.com**